UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES FOR AN ORDER (1) AUTHORIZING THE USE OF A PEN REGISTER AND A TRAP AND TRACE DEVICE AND (2) AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION AND/OR CELL SITE INFORMATION.

MEMORANDUM AND ORDER

M 05-1093 (JO)

----------X

JAMES ORENSTEIN, Magistrate Judge:

The United States seeks reconsideration of my earlier order in this matter, reported at 384 F. Supp.2d 562 (E.D.N.Y. 2005) (the "August Order"), denying its application for the "disclosure of the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call, for the Subject Telephone." Renewed Sealed Application ("Application") at 1-2. Such applications are normally considered *ex parte*, but in light of the novelty of the issue and the absence at the time the August Order was written of any published case law, I have also allowed *amicus curiae* the Electronic Frontier Foundation ("EFF") to submit a letter-brief in opposition to the instant motion. Having considered all of the arguments as well as the intervening decision in *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 2005 WL 2656621 (S.D. Tex. Oct. 14, 2005) ("*Cell Site*"), I conclude that at least some of the government's objections to the August Order's reasoning are well taken, and therefore grant the motion to reconsider. On reconsideration, as explained below, I conclude that existing law does not permit the government to obtain the requested information on a prospective, real-time basis without a showing of probable cause. I therefore again deny the government's application.

I. Background

On a motion for reconsideration, I would normally start the discussion of background facts and procedural history with a disclaimer assuming the reader's familiarity with the challenged order. Not so here: having gotten at least one thing dead wrong in the August Order, *see* n.4, *infra*, I will optimistically assume the reader's ignorance rather than continue to advertise my own. I therefore proceed essentially from scratch.

A. The Initial Application And Proposed Orders

On August 23, 2005, the government simultaneously filed three documents, all of which remain under seal: an application for certain relief, a proposed order authorizing law enforcement agents to take certain investigative steps with the compelled assistance of the relevant provider of telecommunications services (the Sealed Order of Authorization, or "Authorization Order"), and a complementary separate order directed to the provider itself (the Sealed Order to Service Provider, or "Provider Order"). Because portions of each document are relevant to the discussion below, I reproduce those portions here.

1. The Application

The government's application explicitly sought three forms of relief, and cited the specific statutory authority on which it relied for each:

> 1. Pursuant to 18 U.S.C. §§ 3122 and 3123, [an order] authorizing the continued installation and use of a pen register and the use of a trap and trace device for a period of sixty days ... on the [Subject Telephone;][1]

[1] The original application sought renewal of authority previously granted by a different magistrate judge. That fact that the matter came before me by way of a request for renewal has no bearing on my analysis, and the government has not suggested that it should. The "Subject Telephone" was of course identified in the sealed application but that information properly remains under seal and likewise has no bearing on my analysis.

> 2. Pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(c)(2) and 2703(d), [an order] directing continued disclosure of subscriber information for all published, non-published, or unlisted numbers dialed or otherwise transmitted to and from the Subject Telephone, upon oral or written demand by [the relevant law enforcement officers]; and
>
> 3. Pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), [an order] directing continued disclosure of the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of the call, for the Subject Telephone.

Application at 1-2.

In support of the application to continue using the pen/trap devices,[2] the prosecutor made the requisite certifications under the Pen/Trap Statute, *see* 18 U.S.C. § 3122(b), and in fact went beyond the requirement of a bare-bones certification "that the information likely to be obtained is relevant to an ongoing criminal investigation," *id*. § 3122(b)(2), by explaining the basis for that certification. Application at 3-4. The prosecutor next went on to recite the basis for the remaining requests under the SCA by providing "specific and articulable facts showing that there are reasonable grounds to believe that the subscriber information pertaining to telephone numbers identified through the pen register and trap and trace device on the Subject Telephone

---

[2] For ease of reference, I will use the following shorthand terminology: "pen/trap devices" refers to either or both of a pen register or a trap and trace device; "Pen/Trap Statute" refers generally to Chapter 206 of Title 18 of the United States Code (including sections 3121 through 3127) ("Pen Registers and Trap and Trace Devices"); the "SCA" or "Stored Communications Act" refers generally to Chapter 121 of Title 18 of the United States Code (including sections 2701 through 2712) ("Stored Wire and Electronic Communications and Transactional Records Access"); "Title III" refers generally to Chapter 119 of Title 18 of the United States Code (including sections 2510 through 2522) ("Wire and Electronic Communications Interception and Interception of Oral Communications"); "ECPA" refers to the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); and the "PATRIOT Act" refers to the USA PATRIOT Act (the acronymic full title of which I omit), Pub. L. No. 107-56, 115 Stat. 272 (2001).

and cell site information regarding the Subject Telephone will be relevant and material to an ongoing criminal investigation[.]" *Id*. at 5; *see id*. at 5-7 (reciting facts).

The Application then went on to make several requests for relief that added detail to the earlier requests to use pen/trap devices and secure subscriber information. For reasons that will become clear, the structure of those requests is pertinent, and I summarize them here. First, in a multi-part paragraph generally purporting to rely on provisions of the SCA, the government requested that the court issue an order authorizing (a) the continued installation and use of a pen register, (b) the continued installation and use of a trap and trace device, and (c) an additional request not pertinent to the instant matter made "pursuant to 18 U.S.C. § 3123(b)(1)(C)." Application at 7-8. Nothing in the paragraph referred to cell site authority.

The remaining requests all sought orders compelling assistance from telecommunications service providers. Specifically, the government sought orders directing the relevant providers (a) to notify government agents of service changes for the Subject Telephone; (b) "[p]ursuant to 18 U.S.C. § 3123(a)(1) and § 3123(b)(2)," to furnish appropriate assistance to the installation and use of the pen/trap devices; (c) to "furnish the results of the pen register and trap and trace installations to [government agents] as soon as practicable, and on a continuing basis ... for the duration of the order[;]" and (d) "not to disclose the existence of this order or the pen register and cell site location authorization" or other associated information to any person absent a court order. Application at 9-11. Thus, although the Application did request "disclosure" of prospective cell site information in its general request for relief at the beginning of the document, it did not request an order directing any service provider to furnish such information in the detailed prayer for relief at the end of the document, and did not in any manner specify who was

supposed to make the requested "disclosure." Nevertheless, as discussed below, the proposed Authorization and Provider Orders did include language requiring such assistance.

2. The Authorization Order

The proposed Authorization Order included both findings and several specific orders. The proposed findings closely tracked the three requests for relief at the beginning of the Application:

> Pursuant to 18 U.S.C. § 3123, Applicant has certified that the information likely to be obtained by such use [of pen/trap devices] is relevant to an ongoing criminal investigation....
>
> Pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(c)(2) and 2703(d), Applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that subscriber information for [numbers gleaned from the pen/trap devices] is relevant and material to an ongoing criminal investigation ...
>
> Pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), Applicant has further established that there are specific and articulable facts showing that there are reasonable grounds to believe that cell site information is relevant and material to an ongoing criminal investigation....

Authorization Order at 1-2; *cf.* Application at 1-2.

On the basis of those findings, the Authorization Order proposed nine specific orders. The first two authorized law enforcement agents, "pursuant to 18 U.S.C. § 3123," to continue the installation and use of pen/trap devices, including for purposes of recording or decoding "dialing, routing, addressing or signaling information." The third required relevant service providers, "pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(c)(2) and 2703(d)," to provide subscriber information about the numbers obtained from the use of the pen/trap devices. The fourth – the denial of which is at issue in this litigation – required, "pursuant to 18 U.S.C. §§ 2703(c)(1)(B),

2703(c)(2) and 2703(d), that the wireless carriers shall provide" cell site information. Authorization Order at 2-4.

The fifth specific order provided that "this authorization for the continued installation and use of a pen register and trap and trace device" applies to the Subject Telephone even after any changes in the number assigned to the same instrument, under certain conditions – but it did not provide for such continued authorization as to cell site information. The sixth specific order complemented the fifth by requiring service providers to notify the government agents about relevant service changes to the Subject Telephone. Authorization Order at 4-5.

The seventh and eighth specific orders imposed obligations on the service providers relating only to the pen/trap devices and made no mention of cell site information: the former required service providers to furnish agents with all information and assistance necessary to accomplish the devices' installation and use, and the latter required providers to furnish the results of the devices' use to agents as soon as practicable and on a continuous basis. Finally, the ninth specific order directed the investigating agency to compensate service providers for certain expenses and the tenth provided for appropriate secrecy and sealing. Authorization Order at 5-6.

In sum, the Authorization Order, like the Application, cited only the SCA – and not the Pen/Trap Statute – in connection with the disclosure of cell site information. The Authorization Order likewise directed the relevant carriers to provide cell site information but did not refer to the disclosure of such information in the specific directions regarding changes to the Subject Telephone, the furnishing of assistance, or the speedy and continuous disclosures of information during the pendency of the order.

3. The Provider Order

The Provider Order contained one "whereas" clause followed by eleven specific orders. The latter were essentially verbatim repetitions of the specific orders in the Authorization Order, and I therefore do not describe them at length here. The former recited that the court had "entered an order pursuant to Title 18, United States Code, §§ 3121-26 and § 2703(d) authorizing the use of a pen register [with cell site location authority] and a trap and trace device for a period of sixty days from the date of this order on" the Subject Telephone. Provider Order at 1 (brackets in original). The phrasing suggests that the only cell site information the government contemplated obtaining as a result of the Authorization Order would be prospective (*i.e.*, pertaining to calls not yet made at the time of the order), rather than the disclosure of actual records held by the service providers about previously made calls. The phrasing further suggests that the prospective cell site information the government sought would be obtained via the pen register – and thus, by negative inference, not by means of a separate disclosure of information by the service provider. As the Provider Order specified that government agents would "install, or cause to be installed" the pen register, Provider Order at 1, it thus appears that the government contemplated obtaining the requested cell site information by means of the authorized investigative actions of its agents rather than by the actual disclosure of records or information held by any service provider.

B. Procedural History

The government submitted the Application and proposed orders *ex parte* on August 23, 2005. On August 25, 2005, I signed the proposed orders but struck out in each the paragraph directing the service providers to disclose cell site information (and also, in the "whereas" clause

of the Provider Order, the bracketed reference to "cell site location authority"). The same day, I issued the August Order to explain the reasons for that outcome.

On September 9, 2005, the government filed a document styled "Notice of Appeal." Docket Entry ("DE") 3. Although the document itself does not specify whether the appeal is being taken to the district judge on miscellaneous duty in this district's Long Island courthouse or to the United States Court of Appeals, the docket entry information that the government provided upon electronically filing the document described it as a "Notice of Appeal of a Magistrate Judge's Decision to a District Judge (on a mj case)." DE 3. Later the same day, the government filed a letter-motion asking me to reconsider the August Order. DE 4 (the "Motion").

On September 16, EFF sent me an unsolicited letter requesting leave to file a brief in opposition to the government's motion as *amicus curiae*. DE 5. Having already come to the view that I would benefit from adversarial testing of the government's arguments on the novel legal issue presented,[3] I granted EFF's application. DE 6. EFF thereafter submitted its letter in response to the government's Motion on September 23, 2005. DE 7 (the "Response").

After several delays (most of which were authorized, *see* DE 8-DE 9 and orders endorsed thereon), the government submitted its reply to the EFF Response on October 11, 2005. DE 12 (the "Reply"). As of that time, when all of the briefs on the instant matter had been submitted, my August Order was the only published federal court decision on the propriety of governmental applications for cell site information based on a showing less exacting than probable cause. Luckily, that was about to change.

---

[3] As the government is aware, shortly before receiving EFF's application, I had contacted a representative of a local bar group to inquire if it would be interested in submitting an *amicus* brief. The EFF's action mooted the inquiry.

C. The Intervening *Cell Site* Decision

On October 14, 2005, the Honorable Stephen Wm. Smith, United States Magistrate Judge for the Southern District of Texas, issued a decision resolving virtually the same issue now before me:

> what legal standard the government must satisfy to compel the disclosure of ... prospective or "real-time" cell site data. More particularly, is this location information merely another form of subscriber record accessible upon a showing of "specific and articulable facts" under 18 U.S.C. § 2703(d), as the government contends? Or does this type of surveillance require a more exacting standard, such as probable cause under Federal Rule of Criminal Procedure 41?

Cell Site, 2005 WL 2656621 at *2.

I say the issues are "virtually the same" rather than "identical" advisedly: although the government's statutory arguments to Judge Smith were essentially the same as those now made to me, the application at issue in the Texas case was not identical to the one here. In particular, the scope of the cell site information sought in Texas may have been materially different from the information sought here. As noted above, the Application before me sought "disclosure of the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and if reasonably available, during the progress of a call, for the Subject Telephone." Application at 1-2. The Texas application made the same request, but also sought "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture." *Cell Site*, 2005 WL 2656621 at *1. It may be that the government contemplated that a grant of the Application in the matter before me would implicitly authorize it to get the additional information explicitly

requested in the Texas matter, but I assume otherwise, as the government manifestly knows how to make explicit its intention to seek such authority.

As will become evident in the discussion below, any such difference between the two applications may be critical to a determination of whether the disclosure of cell site information implicates the rules applicable to a "tracking device" as defined in 18 U.S.C. § 3117(b). That is because the additional information requested in Texas might enable law enforcement agents to engage in "a process of triangulation from various cell towers," and thereby "track the movements of the target phone, and hence locate a suspect using that phone." *Cell Site*, 2005 WL 2656621 at *3 & n.5 (citing Darren Handler, Note, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative,* 10 Va. J. L. & Tech. 1, at *8, *17-*21 (Winter 2005); Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators,* 18 Harv. J. L. & Tech. 307, 308-16 (Fall 2004)).

In a meticulous and persuasive opinion, Judge Smith first described the technological and statutory matrix in which the instant issue arises, and then went on to explain why the government's position is untenable. Specifically, Judge Smith concluded that the disclosure of cell site information turns a mobile telephone into a "tracking device" and therefore such disclosure may not be authorized without a showing of probable cause. *Id*. at *5-*9. Judge Smith also considered and rejected the government's contention that, independent of the tracking device statute, cell site information is available pursuant to a less exacting showing either under the SCA alone, *id*. at *9-*12, or pursuant to a hybrid application invoking both the SCA and the Pen/Trap statute. *Id*. at *12-*15. As will become apparent, Judge Smith's analysis has made my job in the instant case considerably easier, but it does not resolve all of the issues before me.

II. Discussion

A. Procedural Issues

Before addressing the substantive issues on which *Cell Site* provides invaluable guidance, I must first clear some procedural hurdles that were not presented in the Texas case.

1. Reconsideration In General

a. Is Reconsideration Available?

There is no specific rule, either in the Federal Rules of Criminal Procedure or in this court's Local Criminal Rules, providing for the reconsideration of a ruling on a criminal matter. Moreover, while the court has explicitly made many of its Local Civil Rules applicable to criminal cases, the specific rule governing motions for reconsideration, Local Civil Rule 6.3, is not among those so incorporated. *See* Loc. Crim. R. 1.1(b) (incorporating Loc. Civ. R. 1.2 through 1.10, 39.1, 58.1, and 67.1). Accordingly, there is good reason to conclude that the Board of Judges of this district has deliberately chosen *not* to permit motions for reconsideration in criminal matters. Given the general disfavor with which motions for reconsideration are viewed in the civil context, such a choice would hardly be unreasonable in the context of criminal cases, where courts are hard pressed, even without such motions, to give defendants, the government, and the public the speedy trials that the law requires.

Nevertheless, such motions are made in criminal cases, and courts in this district have resolved them according to the same principles that apply in the civil context. *See*, *e.g.*, *United States v. RW Professional Leasing Services Corp.*, 327 F. Supp.2d 192, 196 (E.D.N.Y. 2004) (citing *Dellefave v. Access Temps., Inc.*, 2001 WL 286771, at *1 (S.D.N.Y. Mar. 22, 2001); *In re Houbigant, Inc.*, 914 F. Supp. 997, 1001 (S.D.N.Y. 1996)); *United States v. Avellino*, 129 F.

Supp.2d 214, 217 (E.D.N.Y. 2001) (granting reconsideration without discussion of standard of review); *United States v. Mosquera*, 816 F. Supp. 168 (E.D.N.Y. 1993). The same is true in other federal jurisdictions, and the Supreme Court appears to have condoned the practice, albeit without directly ruling on the source of authority for it. *See*, *e.g.*, *United States v. Ibarra*, 502 U.S. 1, 4 (1991). The salutary practice avoids needless appellate litigation in those cases where a court can readily recognize and correct its own errors. Moreover, the concern about speedy trials is not present in the context of this criminal matter – which in any event is technically considered a "miscellaneous" one because it has been given neither a civil nor a criminal docket number, *see* Loc. R. 50.1(a), (e) – where no defendant has been charged. Accordingly, I will assume that I have the authority to reconsider my earlier decision at the government's request, notwithstanding the absence of an explicit rule to that effect.

b. The Standard of Review

The standard of review applicable to a motion for reconsideration under the civil rules that the government cites by analogy is a familiar one:

> This standard is "strict." *Shrader v. CSX Transp., Inc.*, 70 F.3d 255, 257 (2d Cir. 1995). Such motions are committed to the "sound discretion of the district court," *see McCarthy v. Manson*, 714 F.2d 234, 237 (2d Cir. 1983), and the burden is on the movant to demonstrate that the Court overlooked controlling decisions or material facts that were before it on the original motion, and that might "materially have influenced its earlier decision." *Anglo Am. Ins. Co. v. CalFed, Inc.*, 940 F. Supp. 554, 557 (S.D.N.Y. 1996). The movant may neither repeat "arguments already briefed, considered and decided," nor "advance new facts, issues or arguments not previously presented." *Schonberger v. Serchuk*, 742 F. Supp. 108, 119 (S.D.N.Y. 1990) (citations omitted). Rather he must "point to controlling decisions or data that the court overlooked – matters, in other words, that might reasonably be expected to alter the conclusion reached by the court." *Shrader*, 70 F.3d at 257.

Carione v. United States, 368 F. Supp.2d 196, 198 (E.D.N.Y. 2005).

The prohibition that bars the movant from advancing arguments not previously presented might be deemed sufficient to resolve the instant application, in light of the fact that the government, despite an explicit invitation, initially declined to submit any argument supporting its Application. However, as I noted at the time, the government also purported to reserve the right to present such arguments "in the future, either in seeking review of any denial of relief in the instant matter or in connection with other applications." 384 F. Supp.2d at 563.

While I do not endorse such an approach as a routine matter, and do not in any way suggest that the tactic suffices to supersede the case law barring such piecemeal litigation, I nevertheless consider the government's arguments as if properly before me for two reasons. First, the instant issue is an important one that is ripe for decision and affects the daily business of this court; judicial economy is therefore advanced rather than frustrated by reaching the merits here. Second, even without the prompting of the new arguments set forth in the government's motion, I would deem reconsideration appropriate on the ground that I have noted relevant law that I overlooked in my initial decision, namely, 18 U.S.C. § 2510(8).[4]

---

[4] I began my analysis in the August Order by assuming that the "only" provision of 18 U.S.C. § 2703 pertinent to the government's application was the portion of subsection (d) permitting the disclosure of "the contents of a wire or electronic communication." 384 F. Supp.2d at 563. There may be many statutory labels than can arguably be applied to cell site information, but "contents of a wire or electronic communication" is not one of them. *See* 18 U.S.C. § 2510(8) ("'contents,' when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). Moreover, as the government has since made clear, its reliance on § 2703 is predicated on the provisions allowing for the disclosure of "a record or other information pertaining to a subscriber to or customer of [electronic communication] service (not including the contents of communications)." 18 U.S.C. § 2703(c)(1); *see* Motion at 3-4. The irony of having made so wrong a turn at the start of an order that ended with a paean to late-found wisdom, 384 F. Supp.2d at 566 (citing *Henslee v. Union Planters Nat. Bank & Trust Co.,* 335 U.S. 595, 600 (1949) (Frankfurter, J., dissenting)), is not lost on me. If wisdom is the guest who too often never comes, carelessness is apparently the one who ignores all hints that it is time to go.

2. Timeliness

I consider the motion for reconsideration to have been timely filed. Assuming the government may properly seek reconsideration by analogy to applicable civil rules (*see* Fed. R. Civ. P. 59(e); Loc. Civ. R. 6.3), it had ten days, excluding intervening weekends and holidays, to file its application. *See* Fed. R. Civ. P. 6(a); Loc. Civ. R. 6.3-6.4; *see also* Fed. R. Crim. P. 45(a)(2) (similar computation rule in criminal cases); Loc. Crim. R. 45.1. Applying that rule, September 9, 2005, was the last day on which the government could seek reconsideration by analogy to the local civil rules. I therefore need not resolve the government's dubious suggestion that a motion for reconsideration of a ruling on a criminal matter may be timely if made within 30 days of the original ruling. *See* Motion at 1-2 n.1 (citing *Canale v. United States*, 969 F.2d 13 (2d Cir. 1992); *United States v. Gross*, 2002 WL 32096592, *1-*3 (E.D.N.Y. Dec. 5, 2002)).

3. The Effect Of The "Notice Of Appeal"

As noted above, the instant motion for reconsideration was filed *after* the government filed its Notice of Appeal (twelve minutes after, according to the docket). If that Notice had been an appeal to the Second Circuit of a final order of the district court, it would be "an event of jurisdictional significance [that would divest] the district court of its control over those aspects of the case involved in the appeal." *Motorola Credit Corp. v. Uzan*, 388 F.3d 39, 53 (2d Cir. 2004) (citing *Griggs v. Provident Consumer Discount Co.*, 459 U.S. 56, 58 (1982)); *see also* 28 U.S.C. § 1291.

I assume that the government's description of the Notice in its docket entry clarifies any ambiguity in the document itself, and that the Notice is in fact meant to trigger review by a district judge of my order, and that in doing so, it is again relying on an analogy to civil practice –

in this case, Fed. R. Civ. P. 72. Viewed in that light, the Notice does nothing to divest me of the power to decide the instant motion, as there is no rule analogous to that in *Motorola* that divests a magistrate judge of authority to act as to matters under review by a district judge (although judicial economy of course counsels against parallel proceedings on the same issue before both).

I assume that the government's actions in this respect are a form of insurance against the possibility that in the time between the issuance of this decision and the time it's attorneys become aware of it, the time to seek review by the district judge on miscellaneous duty will lapse. Thus, in theory, upon the issuance of this decision, the already-filed Notice of Appeal will take immediate effect, thereby preserving the right to seek review on the basis of a supporting brief to be submitted later. I have no need to opine on the need for or effectiveness of such procedures; I note only that they do not appear to deprive me of the authority to determine the motion now before me.[5]

4. Potential Mootness

The government's original application sought relief over a 60-day period. I granted partial relief on August 25, 2005, meaning that the government's ability to obtain the requested cell site information would have expired in any event on October 24, 2005. The instant decision

[5] When I was moments away from issuing this order, the government submitted an application seeking, "[f]or good order's sake," permission to withdraw the Notice of Appeal upon the grant of an extension of time to seek review of "the impending decision of the motion for reconsideration. DE 15. I agree that "it would not be conducive to orderly judicial review to require the government to file objections the same day as the motion will be decided." *Id*. at 2. Therefore, by analogy to my authority under Fed. R. Civ. P. 6(b)(1), I enlarge by five business days the government's time to seek review by the miscellaneous duty judge. The government must therefore submit its objections to this decision no later than October 31, 2005. On the basis of that order, I deem the Notice of Appeal to be withdrawn.

is therefore made at a time when, at least in theory, a different outcome could afford the government at least minimal relief. It is therefore not moot.[6]

To the extent that the issuance of this order does, as a practical matter, come so late that a different outcome would not in fact afford the government any meaningful relief, I nevertheless conclude that the matter is not moot. The difficulty of completing the litigation before me and review by higher courts within the 60-day period may well suggest the applicability of a recognized exception to the "case or controversy" requirement that applies to circumstances that are capable of repetition while evading review. Specifically, the government's disagreement with my ruling relates to a proposed course of action that "was in duration too short to be fully litigated prior to its cessation or expiration, and ... there is a reasonable expectation that the same ... party will be subjected to the same" denial of the same proposed action again in future applications. *United States v. Quattrone*, 402 F.3d 304, 309 (2d Cir. 2005) (citations and internal quotations omitted).[7]

---

[6] The jurisdictional mootness issue is arguably non-existent if the application for cell site information is viewed as a free-standing request for relief that may be granted at any time. If the government were seeking only historical cell site information, that would of course be correct (though of course in such circumstances there would be no issue to resolve, as § 2703(d) plainly allows such relief). But as the Application and the proposed orders indicate, the government seeks to obtain the cell site information it wants by means of the pen register I have permitted it to install and use during the 60-day period that is about to expire. Thus, were I to grant the authority the government seeks tomorrow, it would have authority to obtain the information but no authority (absent renewal of the pen register, which is not before me) to use the device by which the information is to be obtained.

[7] Of equal concern, though not a matter I can resolve, is whether the government can effectively seek review of my decision if the matter becomes moot within minutes or hours of its issuance. It may be that the lapsing of the 60-day period precludes such review under the usual interpretation of the Constitution's "case or controversy" requirement, *see* U.S. Const. Art. III, § 2, but that is not my intention. As stated in my original order, I and other magistrate judges would benefit from more authoritative guidance. *See* 384 F. Supp.2d at 566; *see also Cell Site*,

B. The Legal Landscape

Having cleared the procedural underbrush, I can now begin to take full advantage of (*i.e.*, plagiarize) the *Cell Site* opinion. To the extent I follow the latter decision's lead, it is not because I view it as controlling, nor even because I am simply deferring to persuasive precedent (although it is assuredly that). Rather, my reliance reflects the fact that I have considered precisely the same statutes and legislative history as Judge Smith (and apparently many of the same arguments), and have independently arrived at the same conclusions as did he. Having done so, it is simply a matter of efficiency to cite or quote from his decision rather than reinvent the wheel.

As Judge Smith carefully demonstrated,

> Despite frequent amendment, the basic architecture of electronic surveillance law erected by the ECPA remains in place to this day. This statutory scheme has four broad categories, arranged from highest to lowest legal process for obtaining court approval:
>
> - wiretaps, 18 U.S.C. §§ 2510-2522 (super-warrant);
> - tracking devices, 18 U.S.C. § 3117 (Rule 41 probable cause);
> - stored communications and subscriber records, 18 U.S.C. § 2703(d) (specific and articulable facts);
> - pen register/trap and trace, 18 U.S.C. §§ 3121-3127 (certified relevance).

Cell Site, 2005 WL 2656621 at *4-*5.

2005 WL 2656621 at *16 (expressing "the full expectation and hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis").

I need not replicate Judge Smith's detailed explanation, but it is instructive and persuasive authority on which I rely and to which I invite the reader's attention. For present purposes, it suffices simply to explain the parenthetical shorthand phrases quoted above. As Judge Smith noted, the statutory regime establishes four progressively more burdensome levels of legal process through which the government must go to obtain progressively intrusive types of surveillance authority.

The least exacting process is the certification required to obtain permission to use pen/trap devices: a prosecutor need only certify that the information to be obtained via pen/trap devices "is relevant to an ongoing criminal investigation" and a court must thereupon grant the request. *See Cell Site* 2005 WL 2656621 at *4 (citing 18 U.S.C. § 3122(b)(2); *id*. § 3123(a)(1), (2); J. Carr & P. Bellia, *The Law of Electronic Surveillance* § 1:26, at 1-25 (West 2004)).

The next level of process is required when the government seeks access to any "record or other information pertaining to a subscriber to or customer of [electronic communication] service (not including the contents of communications)." 18 U.S.C. § 2703(c)(1). To obtain such disclosure, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The next level of burden is the familiar probable cause standard under Rule 41 that applies generally to applications for search warrants. Judge Smith also concludes that that level of process applies when the government seeks to install a tracking device, as defined in 18 U.S.C. § 3117(b), an issue I address below in Part F of this discussion.

Finally, Judge Smith's reference to a "super-warrant" requirement applicable to governmental requests for authorization to conduct wiretaps alludes to certain specific requirements of Title III. In many ways, an application to intercept the contents of communications parallels a traditional warrant application: it must establish probable cause to believe that particularly described evidence of a specific crime will be found by giving the government leave to search a particularly described place. In the case of a wiretap, the evidence is the contents of communications and the "place" to be searched is, in essence, a telephone line. But Title III also requires additional showings not necessary to obtain a more traditional warrant: in particular, the applicant must demonstrate that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous[.]" 18 U.S.C. § 2518(3)(c). It is this additional requirement – that a wiretap be a technique of last resort – that makes the Title III standard a "super-warrant" showing.[8]

It is against this statutory backdrop that I assess the government's efforts to secure authorization to obtain cell site information on a showing less exacting than probable cause, as well as the EFF's suggestion that such information requires a showing comparable to Title III's super-warrant requirement.

---

[8] The opinion in *Cell Site* also refers to other aspects of the Title III application procedure in explaining the "super-warrant" description. 2005 WL 2656621 at *3. However, those other aspects – the restricted class of crimes to which the statute applies, the time- and subject-matter restrictions on interceptions, the requirement of notice to targets, and the heightened judicial oversight (as well as the requirement of high-level approval for the application within the Department of Justice, *see* 18 U.S.C. § 2516(1)) – are all, in my view, either analogous to aspects of a traditional search warrant or related to the procedural burden on the applicant without changing the substantive showing the applicant must make. The "last resort" requirement, however, plainly does require the government to prove something in seeking a wiretap that it need not prove in seeking a traditional search warrant.

C. A Certification Of Relevance Under The Pen/Trap Statute Is Insufficient

The government does not assert that it can obtain the prospective cell site information at issue on the strength of a bare certification of relevance under the Pen/Trap Statute. At least I think it does not, though I confess that my conclusion in that regard necessarily rests on a best-two-out-of-three approach to reading the government's submissions. *Compare* Application at 1-2 (seeking cell site information "[p]ursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d)") *with* Motion at 7 ("We do not seek authorization to obtain cell site information based on a mere finding that the government has certified the information's likely relevance.") *and* Reply at 7 ("The Court may therefore reasonably base its authority to order disclosure on a prospective basis entirely on the Pen/Trap Statute").

To the extent my reading of the government's intention is incorrect, I adhere to my earlier conclusion that Congress has prohibited the government from relying on a mere certification of relevance to obtain prospective cell site information through the use of pen/trap devices. As I explained in the August Order:

> Section 103(a)(2) [CALEA] requires each telecommunications carrier to ensure that the telephone service it provides is capable of being used by authorized law enforcement agents for certain investigative purposes. However, the statute explicitly provides that "with regard to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information *shall not include any information that may disclose the physical location of the subscriber* ...." 47 U.S.C. § 1002(a)(2)(B) (emphasis added)....
>
> By its terms, the provision just quoted does no more than govern what a private sector entity must do to assist law enforcement. At the risk of building a straw man, it could thus be argued that CALEA does nothing to prohibit agents from seeking, and courts from granting, authority to obtain cell site location information. There are two flaws with that argument.

First, parsing the statute so finely to achieve such a construction would plainly be at odds with the legislators' intent. In reporting favorably on CALEA, the House Judiciary Committee sought quite emphatically to quell concerns about how the proposed legislation might infringe individual Americans' privacy rights:

> THE LEGISLATION ADDRESSES PRIVACY CONCERNS
>
> Since 1968, the law of this nation has authorized law enforcement agencies to conduct wiretaps pursuant to court order.... The bill will not expand that authority. However, as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.
>
> In the [past] eight years ... society's patterns of using electronic communications technology have changed dramatically....
>
> Therefore, [CALEA] includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill:
>
> ...
>
> 2. Expressly provides that the authority for pen registers and trap and trace devices *cannot be used to obtain tracking or location information*, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information.

H.R. Rep. 103-827 at 17, reprinted at 1994 U.S.C.C.A.N. 3489, 3497 (Oct. 4, 1994) (emphasis added). It is thus clear that Congress intended to regulate not only what telecommunications providers could give, but also what law enforcement agents could "obtain."

384 F. Supp.2d at 565.[9]

---

[9] I went on in the August Order to identify a second basis for the conclusion:

> Second, the provision at issue does not simply prescribe a minimum standard for a carrier's assistance to law enforcement; it also establishes a legal proscription against the carrier providing, by means of a pen register or trap and

D. An Offer Of Specific And Articulable Facts Under Section 2703(d) Is Insufficient

The government's initial application appeared to seek prospective cell site information solely on the basis of its showing of specific and articulable facts pursuant to § 2703, and on reconsideration the government adheres to the view that such a showing alone suffices. *See* Motion at 3-5.[10] As explained below, I disagree.

> trace device, the type of information the government now seeks. That fact alone necessarily suffices as a basis to deny the instant application: of the two orders the government would have me sign, one would merely authorize enforcement agents to obtain the information while the other would oblige the relevant telecommunications carrier to provide it. The legislative history of CALEA forbids the former but its text arguably does not. The statute's text does, however, explicitly forbid the latter. 47 U.S.C. § 1002(a)(2)(B). *As the government identifies no other method for its agents to obtain the information it seeks than to have the carrier provide [it]*, I cannot properly sign either proposed order....

Id. at 566 (emphasis added).

On reconsideration, I believe the highlighted portion of the latter analysis was incorrect. As discussed above, a close reading of the government's Application and proposed orders, as well as of its submissions on reconsideration, make it clear that it contemplates obtaining prospective cell site information by using a pen register, and not through any actual disclosure from a provider of electronic communications service. The error in the "second" part of the analysis, however, does not affect the validity of the first, and I adhere to the view that Congress plainly intended the "location" prohibition in CALEA to regulate not only what a carrier can provide, but also what law enforcement can lawfully "obtain."

[10] I am not certain as to whether the government maintains that position in its Reply, or instead retreats completely to the position, discussed in the next section, that it may rely on the hybrid authority created by the SCA and the Pen/Trap Statute together (rather than by either statute alone). Specifically, the government asserts that "[n]othing within the SCA prevents disclosure of cell-site information on a prospective basis." Reply at 7. It makes that assertion, however, in the midst of an explanation of its hybrid authority theory. *Id*. I have no doubt that the SCA authorizes a service provider's disclosure to law enforcement of historical cell site information, to the extent it maintains such records. *See Cell Site*, 2005 WL 2656621 at *11 n.16. As a result, if the government's argument about the SCA's failure to distinguish between historical and prospective information is valid (a matter I address below in part D.3.a of this discussion), than it need rely on no authority other than the SCA, and in particular need not resort to the hybrid theory addressed below.

1. Judge Smith's Analysis In *Cell Site*

a. The Subscriber's Use Of Electronic Communications Service

The government rests its application for cell site information on the provision of § 2703 that permits the disclosure of "record[s] or other information pertaining to a subscriber or customer of [electronic communication] service (not including the contents of communications)." 18 U.S.C. § 2703(c)(1) (quoted in Motion at 3-4).[11] Judge Smith rejected that position on the ground that prospective cell site information does not "pertain to the subscriber's use of the provider's electronic communication service." 2005 WL 2656621 at *10. He reached that conclusion based on the following syllogism:

1. "Electronic communication service" must involve the transmission of "wire or electronic communications." 18 U.S.C. §§ 2510(15), 2711(1).

2. The acquisition of cell site information does not involve the transmission of "wire or electronic communications."

    a. "Electronic communications" are excluded because:

        i. "electronic communication" excludes "any communication from a tracking device," *see* 18 U.S.C. § 2510(12)(C), and

        ii. the acquisition of cell site information converts a mobile telephone into a tracking device as defined in 18 U.S.C. § 3117.

    b. "Wire communications" are excluded because:

        i. a "wire communication" must involve a transfer of the human voice, *see* 18 U.S.C. § 2510(1), (18), and

[11] The government thus does not take the position that cell site information is available under the SCA because it falls within the scope of § 2703(c)(2). As *Cell Site* demonstrates, the latter position would be untenable. 2005 WL 2656621 at *10.

ii. the transmission of cell site information over a control channel, which is separate from the voice channel used in a mobile telephone call, does not involve the transfer of the human voice. *See United States v. Forest*, 355 F.3d 942, 949 (6th Cir. 2004) ("cell site data clearly does not fall within the definitions of wire or oral communications").

See 2005 WL 2656621 at *5-*7 (explaining why acquisition of cell site information converts a mobile telephone into a tracking device), *10-*11 (explaining the remaining steps of the syllogism).

b. Structural Distinctions Between The SCA And Surveillance Laws

A second and independent reason for Judge Smith's rejection of the government's reliance on the SCA as authority for obtaining prospective cell site information is based on the structural differences between that law and other statutes that explicitly provide for the prospective surveillance of communications. I quote his analysis in full:

> Even more compelling is the structural argument against allowing access to prospective cell site data under the SCA. Unlike other titles of the ECPA, which regulate methods of real-time surveillance, the SCA regulates access to records and communications in storage. As implied by its full title ("Stored Wire and Electronic Communications and Transactional Records Access"), the entire focus of the SCA is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.
>
> Unlike wiretap and pen/trap orders, which are inherently prospective in nature, § 2703(d) orders are inherently retrospective. This distinction is most clearly seen in the duration periods which Congress mandated for wiretap and pen/trap orders. Wiretap orders authorize a maximum surveillance period of 30 days, which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap

orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders. Pen/trap results are ordinarily required to be furnished to law enforcement "at reasonable intervals during regular business hours for the duration of the order." 18 U.S.C. § 3124(b). The wiretap statute authorizes periodic reports to the court concerning the progress of the surveillance. 18 U.S.C. § 2518(6). Again, nothing resembling such ongoing reporting requirements exists in the SCA.

Another notable omission from § 2703(d) is sealing of court records. Wiretap orders and pen/trap orders are automatically sealed, reflecting the need to keep the ongoing surveillance under wraps. 18 U.S.C. §§ 2518(8)(b), 3123(d)(1). The SCA does not mention sealing. Pen/trap orders must also direct that the service providers not disclose the existence of the order to third parties until otherwise ordered by the court. 18 U.S.C. § 3123(d)(2). Section 2705(b) of the SCA authorizes the court to enter a similar non-disclosure order, but only upon a showing of possible adverse consequences, such as "seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(b)(1)-(5).

Taken together, the presence of these provisions in other titles of the ECPA and their corresponding absence from the SCA[12] cannot simply be dismissed as a coincidence or congressional absent-mindedness. Pen registers and wiretaps are surveillance techniques for monitoring communications yet to occur, requiring prior judicial approval and continuing oversight during coming weeks and months; § 2703(d) permits access to customer transaction records currently in the hands of the service provider, relating to the customer's past and present use of the service. Like a request for production of documents under Federal Rule of Civil Procedure 34, § 2703(d) contemplates the production of existing records, not documents that may be created at some future date related to some future communication. That is the most obvious explanation why the SCA makes no mention of surveillance periods, extensions, periodic reporting, or sealing. If Congress had not intended the SCA to be retrospective in nature, it would have included the same prospective features it built into the wiretap and pen/trap statutes.

2005 WL 2656621 at *11-*12.

---

[12] As the *Cell Site* opinion elsewhere notes, the SCA was originally enacted in 1986 as part of the ECPA. 2005 WL 2656621 at *4.

c. The Applicability Of *Cell Site* To This Case

I find both parts of Judge Smith's analysis extremely persuasive. In particular, I agree that cell site information is excluded from the definition of both "wire communications" and "electronic communications," and I further agree that the profound structural differences between the SCA and the electronic surveillance statutes suggest that Congress did not intend the former to be a vehicle for allowing prospective, real-time surveillance of a mobile telephone user's physical location and movements during the course of a call. Nevertheless, I do not simply rest on my agreement with those parts of *Cell Site* for several reasons that I explore below.

2. The *Cell Site* Analysis Applies Regardless Of Whether The Application In This Case Seeks Triangulation Information

To the extent Judge Smith's syllogism relies on the finding that the application before him effectively sought to transform a mobile telephone into a tracking device, I cannot make the same assumption here even if I agree with his legal analysis. That is because the application before Judge Smith explicitly sought permission to obtain not only the location of the cell site through which each mobile telephone call would be processed, but also additional information – "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites," 2005 WL 2656621 at *1 – that might allow the government to triangulate the caller's position. *See id*. at *3. The application before me did not explicitly seek such information, and the government's Motion relies in part on the proposition that its application would provide only limited information about the telephone user's location. *See* Motion at 8 ("Cell-sites only reveal the general vicinity of the person using a cellular telephone and the general direction in which they are moving if they are in transit."); Reply at 11 (quoting *United*

States Telecom Ass'n v. FCC, 227 F.3d 450, 463 (D.C. Cir. 2000) ("*FCC*") (appearing to suggest that the cell site information at issue discloses no more than "the nearest cell site at the start and end of the call").[13] As a result, I must consider whether the application before me likewise implicates the tracking device statute notwithstanding the possibly more limited scope of cell site information the government seeks here.

The question is easily answered in the affirmative, and by the decision in *Cell Site* itself. In that case, the government took the surprising position that even acquiring information about multiple cell sites (thereby possibly allowing triangulation) "does not provide 'detailed' location information." 2005 WL 2656621 at *6. If potential triangulation does not do the trick, I cannot imagine the level of additional detail that the government in *Cell Site* would have acknowledged as sufficient to implicate the tracking device statute. But I need not assay the reasonableness of that position; for purposes of the instant analysis it is enough that the *Cell Site* decision, like my own, gives due consideration to the government's assertion that a tracking device provides greater certainty about an individual's location than does the acquisition of cell site information.

As Judge Smith noted in *Cell Site*, the tracking device statute "does not distinguish between general vicinity tracking and detailed location tracking." 2005 WL 2656621 at *6. Instead, the statute simply defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or thing." 18 U.S.C. § 3117(b). Moreover, as *Cell Site* points out, 2005 WL 2656621 at *7 & n.12, the Department of Justice

---

[13] The government renders the citation to this portion of *FCC* as "227 F.3d at 291." The opinion is reported both at 227 F.3d 450 and at 343 U.S. App. D.C. 278, and the quoted passage is found at page 463 of the former and page 291 of the latter. I will cite exclusively to the report of the decision in the Federal Reporter, Third Series.

itself uses the term "tracking device" to describe a device that acquires "information that will allow [a mobile telephone] properly to transmit the user's voice to the cell tower" and thereby determine "the direction and signal strength (and therefore the approximate distance) of the target phone." U.S. Dep't of Justice, *Electronic Surveillance Manual* at 45 (rev. June 2005) (the "*Manual*"). The reference to a single "cell tower" rather than to multiple sites suggests that this "tracking device" (as the government describes it) relies on no more information than the Application in this case seeks.

In the August Order I wrote the following:

> Based on the government's application, it appears that the [statutory] definition [of "tracking device"] precisely describes the attribute of the Subject Telephone (or such other instrument as actually would produce the requested information) that renders the disclosure of cell site location information relevant and material to the ongoing investigation. As the Application recites,
>
> > the general geographic location of the Subject Telephone derived from cell site information used by the Subject Telephone can be used to corroborate the observations of surveillance agents. More specifically, surveillance agents can compare observations of the user of the Subject Telephone with cell site information in order to verify the identification and location of the user of the Subject Telephone.
>
> Application ¶ 10.
>
> In other words, the requested information is useful in the same way that physical surveillance of the telephone user is useful: it reveals that person's location at a given time. The fact that the requested order would authorize the disclosure of cell site location information, "if reasonably available, during the progress of a call," [Authorization Order] at 4, further suggests that the authorization, if granted, would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant.

384 F. Supp.2d at 564. I adhere to that view on reconsideration,[14] and therefore agree with Judge Smith that the acquisition of cell site information does not pertain to the use of electronic communications service.

3. The Government Does Not Seek Disclosure Of Information By A Provider

With due respect to my colleague, I believe that while the syllogism regarding the relationship between cell site information and the term "electronic communications service" is correct as far as it goes, the analysis is useful only to a certain extent. As noted above, the syllogism leads to the conclusion that prospective cell site information does not "pertain to *the subscriber's use* of the provider's electronic communication service." 2005 WL 2656621 at *10 (emphasis added). But § 2703 does not predicate a court's authority to issue a disclosure order on the applicant's ability to show that the requested information pertains to such "use." Instead, the statute authorizes the disclosure of "information pertaining to *a subscriber to or customer of* such service[.]" 18 U.S.C. § 2703(c)(1) (emphasis added). Thus, while I agree that cell site information does not, for the reasons explained in *Cell Site*, pertain to a subscriber's or customer's use of electronic communications service, I disagree that that finding alone suffices to reject the government's application.

In addition, the government raises an argument here that does not appear to have been addressed in *Cell Site* and that could, if valid, undermine the persuasiveness of the second part of the rationale in that case. Specifically, the government argues that there is no cognizable difference between historical and prospective cell site information because, "in an era of

[14] Part F of this discussion addresses the government's assertion that the installation of a tracking device does not require a showing of probable cause.

electronic communications, every datum communicated electronically is 'retrospective' or 'historical' once it is captured." Reply at 7. For ease of reference, I call this the "instantaneous storage" theory. In essence, the government starts with the proposition, with which I have no quarrel, that a court may properly, under § 2703, compel a provider to disclose historical cell site information about past calls that it currently has in electronic storage. The government then goes on to reason that all it seeks here, in asking for essentially real-time access to prospective cell site information, is more of the same:

> Thus, a court order to a provider to disclose cell-site information at or close to the time that it enters the provider's datastream is prospective in one sense but is otherwise retrospective. It is prospective with respect to the continuing obligation that the order imposes on the provider to turn over data *as it is captured*. That obligation, however, only accrues with respect to cell-site information for a particular time, *after* the provider's network has captured it in the course of processing a call. Thus, the same datum that is prospectively covered by a disclosure order is a "record" by the time that it must be turned over to law enforcement.

Reply at 7 (emphasis in original). In light of the foregoing, I must consider whether the government's instantaneous storage theory suffices to overcome the reasoning in *Cell Site* and justify a different result.

The government's use of statutory construction principles to show that the "Stored Communications Act" authorizes the government to acquire information that has never been stored about a communication that does not yet exist is imaginative, and not entirely without precedent.[15] In *Regina v. Ojibway*, 8 Crim. L. Q. 137 (1965), a reviewing court similarly applied

---

[15] I use the phrase "never been stored" advisedly. Both the SCA and Title III define "electronic storage" as "any temporary, intermediate storage of a *wire or electronic communication* incidental to the electronic transmission thereof[.]" 18 U.S.C. § 2510(17)(A) (emphasis added); *see* 18 U.S.C. § 2711(1). As explained in *Cell Site*, however, the transmission of cell site information via a control channel is not a "wire or electronic communication." 2005 WL

canons of statutory construction to find, contrary to the more pedestrian opinion of the magistrate below, that a pony is within the protected class defined by the terms of the "Small Birds Act." *See Stevens v. City of Louisville*, 511 S.W.2d 228, 230-31 (Ky. App. 1974) (reprinting the wholly fictional *Ojibway* decision). Creative as it is, I find the instantaneous storage theory unpersuasive for at least two reasons.

a. An Order Under Section 2703 Can Apply Only To Information Already In Existence

The government cites no authority for the proposition that a court may issue an order under § 2703(d) (or any other part of the SCA) that is "prospective with respect to the continuing obligation that the order imposes on the provider to turn over data as it is captured[.]" Reply at 7.[16] As I read the statute, it confers no such power. To the contrary, it provides that a court may issue an order requiring the disclosure of records or information on the basis of a prosecutor's showing that the requested items "*are* relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d) (emphasis added). The exclusive use of the present tense – rather than, for example, the phrase "are or may be" – suggests that the items requested must already be in existence. So too does another subsection of the same statute, as the following discussion demonstrates.

Had I granted the Application in its entirety, 60 days later the government would have had a record of the cell site information for all calls made in the interim. But the Application's

---

2656621 at *10-*11. Accordingly, the real-time processing of a mobile telephone call places the call's contents in "electronic storage" for purposes of the statutes, but not its cell site information.

[16] To the extent the government identifies on the Pen/Trap Statute as the source of such authority, it relies on the hybrid theory I address below in part E.

request was not the only way for the government to achieve that result; to the contrary, the SCA plainly provides an alternate mechanism for doing so. Specifically, upon commencing the use of its pen register pursuant to my order, the government could have made a direct request to the provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f)(1). The provider would have been required to comply without the need for a court order. *Id*. Sixty days later, upon the expiration of the pen register authorization,[17] the government could have asked the court to issue an order requiring the disclosure of the cell site information thus preserved on the basis of its showing of specific and articulable facts. 18 U.S.C. § 2703(d). The only difference between the procedure just described and the one the government strives mightily to defend in this case is the difference between the acquisition of historical evidence about a person's movements and the prospective, real-time tracking of that person. To the extent that difference is an important one, Congress has empowered the government to satisfy its investigative needs upon a showing of probable cause, as discussed below in Part F.[18]

Another reason to suspect the validity of the government's instantaneous storage theory is that it proves too much. If it is true that the transmission of cell site information over the control channel used for a given mobile telephone call may be considered "storage" sufficient to bring the information within the scope of § 2703(c)(1), then it must also be true that the transmission of the same call's contents over the voice channel may likewise be considered "storage" sufficient

---

[17] Pursuant to 18 U.S.C. § 2703(f)(2), the required retention may be for as long as 180 days.

[18] Likewise, to the extent that the government seeks the contents of communications but cannot meet the super-warrant requirements of Title III so as to be in a position to acquire them in real time, § 2703(f) appears to establish a gap-filling remedy in conjunction with § 2703(a).

to bring those contents within the scope of § 2703(a).[19] *Cf. United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005). The latter provision permits the disclosure of "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less ... pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ...." 18 U.S.C. § 2703(a). In other words, if the government's reliance on the essentially instantaneous nature of storage is valid, then it can easily bypass the super-warrant requirement applicable to the interception of wire and electronic communications under Title III simply by describing those communications as in "electronic storage" and obtaining a warrant under Rule 41. At the risk of being cavalier, I trust that no explanation is needed of the assertion that such a result would plainly frustrate the intent of Congress in enacting and repeatedly preserving the requirements of Title III that exceed the requirements of Rule 41.

I therefore conclude, contrary to the government's unsupported assertion, that § 2703 does *not* authorize a court to enter a prospective order to turn over data as it is captured. Instead, the statute establishes a mechanism for compelling the disclosure of information existing at the time an order is issued and for compelling the preservation of such information in the period before such an order is obtained.

b. An Order Under Section 2703 Can Only Authorize A Provider's Disclosure Of Information, Not Interception By Law Enforcement

The government's instantaneous storage theory also fails because, even if the cell site information can properly be viewed as entering electronic storage as soon as it is transmitted over

[19] Indeed, the exclusion of control channel transmissions from the definition of "electronic storage" in 18 U.S.C. § 2510(17)(A) makes the latter far more likely than the former.

the control channel, that fact alone does not make it available to the government. Instead, it merely makes the information subject to disclosure by the service provider. But there appears to be no such actual disclosure contemplated here.

As far as I can discern from the original Application and proposed orders, the government purposes to obtain cell site information directly from its own devices and processes, rather than via disclosure from the telecommunications providers. The SCA authorizes the government to "require a *provider* ... to *disclose* a record or other information pertaining to a subscriber to or customer of [electronic communication] service," 18 U.S.C. § 2703(c)(1) (emphasis added), but does not empower a court to allow a law enforcement officer to intercept such information directly.[20] Yet if the government's intent is to secure disclosure of cell site information from the provider rather than to intercept it directly, I cannot find any suggestion in the application papers, or in the briefing on the instant motion, as to how and when that disclosure will be accomplished.

The application papers are to some extent ambiguous: on one hand, the detailed requests for directions to the providers in the Application say nothing about disclosing cell site information and the general request for cell site information seeks "disclosure" of cell site information without saying who is to disclose it; on the other hand, the Authorization and Provider Orders included provisions directing the carrier to provide cell site information. However, I chalk up that ambiguity to a proofreading error.

---

[20] I use "intercept" in the colloquial sense to refer to the acquisition of information essentially in real time during the course of its original transmission – *i.e.* a method of acquisition distinct from a process by which the information is retrieved from a repository. I recognize that the statutory definition of "intercept," 18 U.S.C. § 2510(4), which is essentially identical to my usage, applies only to the "contents" of communications and is therefore technically inapposite to a discussion of cell site information.

Of greater concern is the absence of any indication of how the government would, as a practical matter, obtain "disclosure" of cell site information from the provider after the fact – however quickly – rather than intercept the information by means of its pen register. As Judge Smith has explained, with reference to the government's own manual, *see Cell Site* 2005 WL 2656621 at *2-*3 (citing the *Manual* at 178-79 n.41), the cell site information the government seeks is apparently conveyed via a control channel that is paired with a voice channel when a mobile telephone is used to make a telephone call. A pen register by definition provides access to that control channel, and that is apparently what the government intends in seeking "dialing, routing, addressing or other signaling information ... transmitted from the Subject Telephone" as part of its pen register application. Application at 7-8. Indeed, the government makes clear in its Reply that it contemplates "cell site information entering a service provider's information system and ... being relayed to law enforcement via pen register or trap and trace device" (a process that the government notes can take "several minutes or more"). Reply at 6 n.3.

I can thus easily see how the government would obtain the cell site information it seeks, on close to a real-time basis, via installation and use of a pen register – but that would not be a disclosure by the telecommunications provider, and therefore not authorized by the SCA. On the other hand, while the SCA might not impose a minimum time limit on how long a provider must "store" a record before disclosing it, there is no hint in the government's papers that any such disclosure will in fact occur. Instead, the government's argument appears to be that cell site information could *in theory* be quickly "stored" by the provider, who could then *in theory* quickly "disclose" it to government investigators, and that therefore we might as well cut out the theoretical middle man to achieve the same result more efficiently. As a matter of transitive

logic the government is assuredly correct, and as a matter of policy I lack authority to offer any opinion; but as a matter of law I am confident that the government's tacit position is not embraced by any statute now in effect.

E. A Hybrid Application Lacking Probable Cause Is Insufficient

1. Introduction: The Theory As Argued On Reconsideration

The preceding discussion's analysis of individual statutes is necessary for purposes of completeness but does not do justice to what appears to be the government's primary argument on its motion for reconsideration. The government, placing more weight on CALEA's use of "solely" than that single word will bear, *see* 47 U.S.C. § 1002(a)(2), vigorously contends that an application made under the SCA and the Pen/Trap Statute together accomplishes what separate applications under each statute might not. For ease of reference, I will call this argument the "hybrid theory."

In essence, the government argues that the whole of electronic surveillance law is greater than the sum of its parts. The government recognizes that CALEA bars it from seeking to compel a provider to disclose information via a pen register that reveals a mobile telephone user's location "solely pursuant to" the Pen/Trap Statute. However, the government argues, that is not what it is trying to do here. Instead, it asserts that its Application relied on the hybrid authority of *both* the Pen/Trap Statute *and* the SCA to compel the disclosure of cell site information. By so doing, the government says, it not only respected the plain language of the CALEA prohibition, but also overcame the objection I raised in the August Order that "where a carrier's assistance to law enforcement is ordered on the basis of something less than probable cause, such assistance must not include disclosure of a subscriber's physical location." 384 F. Supp.2d at 565.

Although the essence of the hybrid theory is that two statutes together accomplish what neither can alone, the argument more precisely rests on a complex chain of inferences derived from several different legislative enactments:

> The argument proceeds as follows: (1) prospective cell site data falls within the PATRIOT Act's expanded definitions of "pen register" and "trap and trace device" because carriers use cell site data for "routing" calls to and from their proper destination; (2) CALEA amended the law to prevent disclosure of a caller's physical location "solely" pursuant to a pen/trap order, so the government need only have some additional authority besides the Pen/Trap Statute to gather prospective cell site information; (3) the SCA provides that additional authority, because cell site data is non-content subscriber information obtainable upon a "specific and articulable facts" showing under § 2703(d); and (4) completing the circle, cell site data authorized by a § 2703(d) order may be collected *prospectively* by virtue of the forward-looking procedural features of the Pen/Trap Statute. By mixing and matching statutory provisions in this manner, the government concludes that cell site data enjoys a unique status under electronic surveillance law – a new form of electronic surveillance combining the advantages of the pen/trap law and the SCA (real-time location tracking based on less than probable cause) without their respective limitations.

Cell Site, 2005 WL 2656621 at *12 (footnote omitted).

2. Did The Application Here Actually Rely On The Hybrid Theory?

Before assessing the merits of the government's hybrid theory, I pause to consider whether it is properly before me. As noted above, I am dispensing with the standards normally applicable to a motion for reconsideration, and am evaluating the government's arguments as if they had been made when I originally solicited them in connection with the original application. However, even viewed in that light, I cannot help but notice a fundamental disconnect between the hybrid theory now before me and the actual relief the government initially requested. Simply put, the Application did not seek prospective cell site information under some hybrid of the SCA and Pen/Trap Statute; instead, it sought discrete forms of relief on the basis of distinctly

identified statutory provisions. It is one thing to argue that the law, in theory, allows the government to obtain cell site information on the basis of a hybrid application, and I will give that argument serious consideration. It is another thing entirely to rewrite history and pretend that I was presented with a hybrid application on August 24, 2005. As discussed below, I was not.

The government's Application cited the specific authority on which it relied for each of the first two components of the relief it sought: the Pen/Trap Statute alone for purposes of using the pen/trap devices, and certain portions of the SCA alone for purposes of obtaining subscriber information on request. Application at 1-2. So too with respect to the component of requested relief at issue here: in seeking prospective cell site information, the government stated that it was acting "[p]ursuant to 18 U.S.C. § 2703(c)(1)(B) and 2703(d)[.]" Application at 1-2. It simply did not invoke, in addition to the SCA, the supplemental (and assertedly transforming) authority of the Pen/Trap Statute, at least not in any way that was reasonably likely to attract my attention.

Moreover, the government cannot credibly argue that it intended its statutory citations to be cumulative, with all of the cited provisions being meant to support the requests for all three forms of relief. If that were so, there would have been no reason for the government to cite 18 U.S.C. § 2703(c)(1)(B) in the request for cell site location authority after having cited the same provision in the previous paragraph relating to subscriber information.

There is in theory an alternate way of interpreting the Application, but it offers no greater support for the government's current position. After reciting the facts supporting its application for relief under the SCA, the Application recited the following:

> 11. Accordingly, based on the above proffer, *and pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(c), and 2703(d),* because there are reasonable grounds to believe that such information is relevant and material to an ongoing investigation, I request that court [sic] issue an order authorizing:
>
> > a. The continued installation and use of a pen register to record or decode dialing, *routing, addressing, or signaling information ....*

Application at 7-8 (emphasis added). As noted above, the portion of the Application that reiterated and elaborated upon the request for relief did not make any explicit mention of the request for cell site authority. It is thus possible to infer that Paragraph 11(a) – by citing the SCA, asking for permission to use a pen register (which is not a matter covered by the SCA), and explicitly referring to "routing, addressing, or signaling information" (which is redundant, given the definition of "pen register" 18 U.S.C. § 3127(3)) – intentionally conflated the SCA and the Pen/Trap statute and thereby, *sub silentio*, invoked the hybrid theory that the government now makes explicit. Such an explanation may be possible, but it strikes me as extremely unlikely. In the context of an application package of boilerplate documents containing at least one plainly inapt citation and several proofreading errors, some of which I have noted in this order, an honest mistake is far more compelling an explanation than is an assertion that the government deliberately wrote this part of its application with needless (and arguably counterproductive) subtlety.

Finally, it is clear that the only cell site information the government requested was prospective in nature. The general references to "disclosure" of cell site information made no mention of any specific period prior to the Application for which such "disclosure" was requested. And the Provider Order, by referring to a "pen register [with cell site location

authority]," Provider Order at 1 (brackets in original), plainly conveyed the government's expectation that it would obtain the requested cell site information via the pen register – meaning it would do so only with respect to calls yet to be made. Thus there was no continuum of cell site information – stretching from historical records to be disclosed by the provider to the information to be generated by future calls – that would arguably implicate a mix of authorities. The Application instead sought prospective information about future calls only, and only on the questionable basis of the Stored Communications Act. There was nothing "hybrid" about that request, or at least nothing beyond the "hybrid" nature of any application that combines in a single document two distinct requests for distinct forms of relief.

Notwithstanding the government's claim that its current explicit reliance on the hybrid theory serves merely to "dispel" what it allows may have been an initial "lack of clarity on that score," Motion at 5-6, it is apparent that the theory is either an afterthought offered to salvage an application that the government belatedly realized was insufficient as written, or alternatively the theory that the government relied on all along but hesitated to expose to judicial scrutiny.[21]

---

[21] I note that in its discussion of the legal basis for seeking the real-time acquisition of prospective cell site information, the *Manual* presciently assumes that courts will reject reliance on the Pen/Trap Statute and makes the case for reliance on the SCA alone discussed here, but does not – even as late as June 2005 – articulate the hybrid theory now before me. *See Manual* at 42-44. As I noted in the August Order, I was presented with (and approved) a similar application for relief in April 2005 – before the *Manual*'s latest revision. *See* 384 F. Supp.2d at 566.

On a related point, I hasten to add that my critique of the perceived disparity between the original Application and the assertion of the hybrid theory on reconsideration is not intended as a criticism of the altogether professional conduct of the talented prosecutors in this case. Applications for pen registers and other routine investigative techniques requiring judicial authorization are often drafted using forms that have been in use for years and that have slowly accreted new provisions and citations written by others at disparate times. *See*, *e.g.*, *Manual* at 176 (reproducing, for use by prosecutors, standard application forms for various investigative techniques). I therefore do not assume that the prosecutors herein gave careful scrutiny to any

Neither possibility instills much confidence that the theory accurately captures the legislative intent that resulted in the enactment of the relevant laws. Nevertheless, in an abundance of caution, I consider the hybrid theory at face value as if it had been made explicit in the government's initial application.

3. Analysis

The same hybrid theory that is now before me was also presented to the court, and rejected, in *Cell Site*. 2005 WL 2656621 at *13-*15. I invite the reader's attention to Judge Smith's exhaustive analysis there, with which I agree in almost every respect and which I will summarize but not reproduce verbatim. In short, Judge Smith identified six problems with the hybrid theory, some of which go to its various component premises, and the remainder of which expose the fallacy of the overarching endeavor of stitching together disparate laws to achieve a result that none alone permits.

The PATRIOT Act amendment to the Pen/Trap Statute was not intended to repeal the CALEA prohibition against using a pen/trap device to acquire a caller's location. The first criticism of the hybrid theory in *Cell Site* is that "the PATRIOT Act's expansion of pen/trap definitions was intended only to reach electronic communications such as e-mail." 2005 WL 2656621 at *13. As Judge Smith explains, nothing in the statute's legislative history suggests that anyone – including those at the Justice Department involved in the advent of the PATRIOT

---

part of the essentially form application, aside from the discussion of facts arising in the underlying investigation. Nor do I assume that they should have done so or that, in submitting the Application, they should have first made sure that they thoroughly understood and were articulating the legal theory (likely developed by others) relevant to the request for cell site information. A busy prosecutor's office such as the one in this district cannot function that way, and it would be unrealistic for courts to expect otherwise.

Act – contemplated that the addition of "dialing, routing, addressing, and signaling information" to the definition of pen/trap devices would extend the reach of such devices to capture cell site information. Given the explicit prohibition in CALEA and the careful attention historically given in the legislative process to the tension between effective law enforcement and legitimate privacy interests with respect to technological advances, it is likely that "even amidst the other important features of that broad-ranging statute, such an important change in electronic surveillance law would have been noticed by *someone*." *Id*. (emphasis in original).

The amended Pen/Trap Statute may not actually cover cell site information. Although he does not say that the government's argument is necessarily wrong in this respect, Judge Smith does question the government's otherwise unexamined assumption that the new definition of pen/trap devices effected by the PATRIOT Act actually encompasses cell site information. That assumption, which I also made in my August Order, *see* 384 F. Supp.2d at 564, is based on the addition of the words "routing, addressing, and signaling information," to the statutory definition. Judge Smith reads the expanded definition to suggest "that this 'routing, addressing, and signaling' information is generated by, and incidental to, the transmission of 'a wire or electronic communication.'" 2005 WL 2656621 at *13 (citing 18 U.S.C. § 3127(3)). Based on this interpretation, he suggests that the new definition of pen register requires that the information collected be tied to an electronic or wire communication - *i.e.*, "an actual or attempted telephone call." *Id*. Because the transmission of cell site information is not such a communication, he therefore questions whether the new definition has any application to cell site information. *See id*. at *13 n.19 (citing H.R. Rep. 107-236 at 53 (2001) ("orders for the installation of pen register and trap and trace devices may obtain any non-content information – 'dialing, routing,

addressing, and signaling information' – *utilized in the processing or transmitting of wire and electronic communications*.") (emphasis added)). While the concern is a plausible one, I do not rely on it in denying the instant motion because as I read the amended definition, it merely ties the concept of "wire or electronic communication" to the "instrument or facility" to which the pen register relates, and not necessarily to the specific communication that the pen/trap device records or decodes. *See* 18 U.S.C. § 3127(3).

The CALEA prohibition against using a pen/trap device to obtain location information was not intended to amend pre-existing law. A critical step in the government's analysis in support of the hybrid theory as argued to Judge Smith, *see* 2005 WL 2656621 at *12, was that the "solely pursuant to" provision enacted in 1994 as part of CALEA was intended to change the pen/trap regime that ECPA created in 1986. Instead, as Judge Smith explains, "[o]ne of CALEA's main objectives was to allow law enforcement to retain *existing* surveillance capabilities in the face of technological change in the telecommunications field." *Id*. at *13 (emphasis added) (citing Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949 (1996)).

I concur with the explanation in *Cell Site*. *See id*. at *13-*15. Of particular significance is the discussion in *Cell Site* of the relationship between the "solely pursuant to" provision and the provisions of the SCA. Specifically, Judge Smith notes that the FBI's then-director, testifying in support of the proposed legislation, made explicit his understanding that the bill did not change the government's electronic surveillance authority but instead "relate[d] solely to advanced technology, not legal authority or privacy." *Id*. at *14 (citing *Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and*

Services: Hearings Before the Subcomm. on Technology and Law of the Senate Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm., 103rd Cong., 2d Sess., at 2, 28 (statement of Director Freeh) ("Freeh Stmt.")). Moreover, as Director Freeh further testified, it was his understanding that "[a]ll telecommunications 'transactional' information is ... exclusively dealt with in [the SCA]" and that "Congress treats law enforcement's use of pen registers and dialing information differently than 'transactional information' – such as detailed telephone billing information ...." Freeh Stmt. at 27-28.

Finally, as Judge Smith notes, the effective date of CALEA's "solely pursuant to" proviso was delayed for four years after enactment to coincide with the effective date of other assistance provisions, while other provisions in the same law – including the addition of the "specific and articulable facts" standard to § 2703(d) of the SCA – became effective immediately. 2005 WL 2656621 at *14 (citing Pub. L. 103-414, § 111(a), (b)). In sum, "[f]ar from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the Pen/Trap Statute has 'nothing to do with' the SCA, and that transactional information 'is exclusively dealt with in [the latter]." *Id*. at *15.

The SCA does not allow the acquisition of prospective cell site information. Judge Smith noted that he refuted that prong of the government's argument earlier in his opinion, *see id.* (citing *id*. at *9-*12), and I have done the same. *See* Part D, *supra*.

An idea this clever must be an accident. Turning from the hybrid theory's "questionable premises," *id*., to its counterintuitive conclusion, Judge Smith's next critique warrants quotation in full:

> The most glaring difficulty in meshing these disparate statutory provisions is that with a single exception they do not cross-reference one another. The Pen/Trap Statute does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the Pen/Trap Statute; and the CALEA proviso [*i.e.*, the "solely pursuant to" language] does not mention the SCA. CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability. Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way.

Id.

How long has this been going on? The final problem that *Cell Site* identifies in the government's theory is that it is impossible plausibly to identify the moment of the hybrid authority's genesis:

> If as the government contends ... three statutes were necessary for conception, then the statutory authority for this surveillance technique was obviously born *after* the PATRIOT Act amendments of 2001. But this timing undercuts any inference that the CALEA proviso (passed 1994, effective 1998) authorized disclosure of location information under the SCA "specific and articulable facts" standard. What need of subsequent legislation if CALEA already did the trick? On the other hand, if CALEA itself marked the true birth date, then the expanded pen/trap definitions in the subsequent PATRIOT Act are rendered immaterial to the analysis. But without the expanded pen/trap definitions, there is no basis to argue that the Pen/Trap Statute covered cell site data; the old definitions only covered numbers dialed. And without the Pen/Trap Statutes's prospective features, so clearly lacking in the SCA scheme, the statutory underpinnings for monitoring of cell phone location simply collapse.

Id. (footnote omitted).

"Solely" is not solely dependent on the hybrid theory. Although Judge Smith's analysis of the hybrid theory is a lily that needs no gilding, I add one more note to address an argument before me of which *Cell Site* makes no mention. Relying on *FCC*, 227 F.3d at 464, the government essentially argues that rejection of its hybrid theory would impermissibly read the word "solely" out of CALEA. In other words, the government argues that rules of statutory

construction require that there be *some* way to use a pen register application in conjunction with *something* that would permit the acquisition of location information; otherwise, the word "solely" would add nothing to the statute. *See* Reply at 4-5.

The principle is correct but inapposite for the simple reason that the contrived hybrid theory is not the only way to salvage independent meaning for CALEA's use of the word "solely." For example, an application to install a wiretap on a mobile telephone might well seek concurrent authorization to use a pen register and acquire cell site location information. Such a combination of prospective surveillance techniques makes eminent sense. More to the point, it makes perfect sense that Congress would want to allow such usage, realizing that the showing of probable cause on a number of matters necessary to satisfy the super-warrant requirements of Title III would satisfy the privacy-based concern that location information should not be available on a mere certification of relevance. Accordingly, I reject the government's contention that the principle of statutory construction cited in *FCC* necessarily renders valid the hybrid theory at issue here.

The reasoning in *Cell Site* is persuasive, and even before reading it I had independently noticed some of the same flaws in the government's hybrid theory as that opinion discusses, though by no means all of them. I have also noted at least one additional flaw in the government's arguments that *Cell Site* had no occasion to address. For all of those reasons, I reject the government's hybrid theory; to paraphrase Judge Smith's fellow Texan, that chimera won't hunt.

F. The Installation Of A Tracking Device Requires A Showing Of Probable Cause

Thus far I have rejected the government's reliance on the Pen/Trap Statute and the SCA, individually or in tandem, as authority for the relief it seeks, and have also agreed with Judge Smith that the request for such relief in effect seeks the installation of a tracking device. As a result, I find that the government is seeking to install a tracking device on the basis of a showing less exacting than the probable cause requirement that Part G makes generally applicable to requests for warrants to seek and seize evidence. I must therefore next decide whether the government is correct in arguing that "it is not the general rule that a 'tracking device' requires a warrant." Motion at 8 (citing *United States v. Knotts*, 460 U.S. 276 (1983)).

As explained below, I conclude that the government's argument in this regard is incorrect. At a minimum, to the extent the government seeks a judicial imprimatur for its acquisition in real time of prospective cell site information, it must proceed under Rule 41. Moreover, to the extent the government asserts that it can proceed without a warrant, on the ground that no cognizable privacy interest is at stake (a position upon which it can, as a practical matter, act at its own risk), I make no decision for the reasons aptly explained in *Cell Site*.

1. Rule 41

At the risk of taking too simplistic an approach, I view the plain language of Rule 41 as providing a default mode of analysis that governs any matter in which the government seeks judicial authorization to engage in certain investigative activities. The Rule says as much. It first specifies that it "does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances." Fed. R. Crim. P. 41(a)(1). It then goes on to specify who may issue a warrant, and for what purposes. *Id*. R. 41(b), (c). As to the latter,

it specifies that a warrant may issue for, among other things, "evidence of a crime." *Id*. R. 41(c)(1). A court may issue such a warrant only upon a showing of probable cause. *Id*. R. 41(d)(1).

The terms of that rule seem plainly to govern here. The government has submitted an application to me, a judicial officer authorized to issue warrants under Rule 41(b), that seeks permission to acquire what the applicant tells me is evidence of a crime. *See* Application at 4-7. Having now determined, after exhaustive analysis, that the application does not implicate any "statute regulating search or seizure, or … special circumstances," *id*. R. 41(a)(1), I must assume that my authority to grant the government's request is constrained by the probable cause requirement of Rule 41(d)(1).

In so holding, I do not purport to decide that a showing of probable cause necessarily suffices to permit the installation of a mobile tracking device, either as a general matter or in the particular circumstances where such installation is accomplished by installing a pen register and using it to acquire the cell site information transmitted over a control channel. Rather, I decide only that the statutes upon which the government relies to secure the requested relief do not suffice to negate the otherwise default requirement of probable cause imposed by Rule 41(d)(1). There may be other statutes that do so that I have not yet had occasion to consider. It may also be, as EFF argues, *see* Response at 6-9, that there is in fact a *more* exacting showing that the government must make to secure the relief it seeks here. As explained below in Part G of this discussion, I need not and do not decide that question here. Instead, I decide only that if the government seeks to have a court grant it permission to acquire prospective cell site information

in real time, it cannot escape the probable cause requirement on the basis of the arguments made to date.

2. The Right To Privacy

The government and *amicus* disagree about the extent to which, if at all, the real-time acquisition of prospective cell site information implicates the right to privacy. *See* Response at 6-9, Reply at 9-12. I note that *Cell Site* addressed such considerations as follows:

> The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in cell site location data, analogizing such information to the telephone numbers found unprotected in *Smith v. Maryland,* 442 U.S. 735 (1979). The Sixth Circuit rejected that analogy in *United States v. Forest,* 355 F.3d 942, 951-52 (6th Cir.2004). Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge. Sometimes, as in *Forest,* cell site data is triggered by law enforcement's dialing of the particular number. 355 F.3d at 951. For these reasons the Sixth Circuit was persuaded that *Smith* did not extend to cell site data, but rejected the defendant's constitutional claim on the narrower ground that the surveillance took place on public highways, where there is no legitimate expectation of privacy. *Id.* at 951-52 (citing *United States v. Knotts,* 460 U.S. 276, 281 (1983)).
>
> Further support for a recognizable privacy interest in caller location information is provided by the Wireless Communication and Public Safety Act of 1999. Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)). This legislation authorized the deployment of a nation-wide 9-1-1 emergency service for wireless phone users, called "Enhanced 9-1-1." Section 5 of the bill amended the Telecommunications Act to extend privacy protection for the call location information of cell phone users:
>
> > (f) Authority to Use Wireless Location Information.--
> >
> > For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to--

> (1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title), other than in accordance with subsection (d)(4) of this section; ...
>
> 47 U.S.C. § 222(f). In other words, location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.
>
> *For purposes of this decision it is unnecessary to draw the line between permissible and impermissible warrantless monitoring of cell site data.* As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant. Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.

2005 WL 2656621 at *8-*9 (emphasis added).

I concur with the preceding analysis. The dispute before me is one of statutory interpretation, and does not call upon me to resolve competing views of privacy rights under the Constitution. The government may sincerely believe that it is free to engage in warrantless monitoring of cell site information, but it has not attempted to do so here. Indeed, judicial review of that position would likely be available only after the government had engaged in such warrantless monitoring. That has not happened here; instead, the prudent prosecutors of this district have sought judicial authorization for the use of the investigative technique at issue. Now that that authorization has been denied on the basis of the showing of specific and articulable facts made to date, I need not anticipate the government's next step. The government may decide to conduct the monitoring without a warrant, it may seek to make a showing of probable cause

(or to argue that its original showing of specific and articulable facts also serves to establish probable cause), it could conceivably try to formulate new arguments supporting its request on the basis of the less exacting showing, or it might simply do without the information it has sought. The government obviously chooses the first course at its peril, but I have no occasion here to preclude it from doing so or to predict what the outcome will be if it takes that chance.

The government contends that if what it seeks is properly considered a tracking device, it need not show probable cause for authority to use it. To the extent it seeks permission for such use from the court, I disagree, for the reasons stated above. To the extent it takes the position that it needs no such permission, I am not in a position to make a binding determination.

G. The EFF's Suggestion That Only a Super-Warrant Showing Suffices Is Not Properly Before The Court On Reconsideration

Thus far I have largely ignored EFF's *amicus* submission in addressing the government's arguments. That fact should not be taken to suggest either a failure to consider that submission or a lack of appreciation for the considerable effort to which the attorneys representing EFF obviously went to provide me with their valuable input. I have omitted reference to EFF's arguments above so as to focus attention on the government's arguments and the reasons I conclude that they cannot prevail. There is, however, one matter raised in the *amicus* submission that warrants explicit attention: namely, EFF's argument that the government's real-time acquisition of prospective cell site information requires satisfaction of a standard comparable to the super-warrant requirement under Title III. Although both EFF and the government have taken pains to brief the issue, I may not properly address it here.

The Application that the government initially submitted to me sought leave to acquire prospective cell site information on the basis of a showing of specific and articulable facts. In denying that application, and in denying the instant motion for reconsideration, I necessarily considered whether the government's showing is sufficient under relevant law. As part of that analysis, I concluded that granting the government's application would be tantamount to authorizing the installation of a tracking device. As a result, I was properly called upon to assess the government's claim that a court may authorize the latter on a showing of less than probable cause – a claim that, as explained above, I reject.

Having done all that, I have completely resolved the issues raised by the instant motion for reconsideration (save only the potential applicability of the All Writs Act, to which I next proceed).[22] Accordingly, any opinion I might offer on the arguments regarding the need for a super-warrant showing would be purely advisory, and therefore inappropriate. My decision that the government's showing of specific and articulable facts is insufficient to permit the real-time acquisition of prospective cell site information does not inherently obligate me to determine what level of proof would be sufficient, and since it resolves the motion before me, that decision does not permit me to go further.

H. The All Writs Act Does Not Provide Sufficient Supplemental Authority

In the foregoing analysis, I have addressed the arguments on reconsideration regarding each of the four levels of legal process that *Cell Site* aptly describes as "the basic architecture of

[22] That would not be the case if the government had pressed me to consider its showing of specific and articulable facts as being sufficient, on the basis of the facts shown, to meet the probable cause requirement and if I had agreed with that position. In such circumstances, there would be a live controversy for me to resolve as to whether a showing of probable cause is sufficient.

electronic surveillance law" that "remains in place to this day." 2005 WL 2656621 at *4. The government's reply, however, asks me to consider yet one more potential source of authority for the relief it seeks: the All Writs Act, 28 U.S.C. § 1651. The government argues, in essence, that the All Writs Act serves here as a mechanism for the judiciary to give it the investigative tools that Congress has not. *See* Reply at 8-9.

There may be contexts where such a use of the All Writs Act is appropriate, and the government cites several specific examples to that effect. *Id*. (citing *United States v. Mosko*, 654 F. Supp. 402, 405 (D. Colo. 1987) (pre-ECPA order authorizing pen register); *United States v. Doe*, 537 F. Supp. 838, 839 (E.D.N.Y. 1982) (order requiring disclosure of telephone toll records to promote the search for a fugitive); *In re Application of the U.S.A. for an Order Directing X to Provide Access to Videotapes*, 2003 WL 22053105 (D. Md. Aug. 22, 2003) ("*Videotapes*") (order requiring future production of then-unrecorded video tapes from a security camera installed in an apartment hallway)). I do not in any way question the correctness of the cited decisions in concluding that they do not advance the government's cause here.

First, all three decisions are distinguishable in critical ways. *Mosko* was decided on the ground that the issuance of a pen register prior to the enactment of ECPA (which prohibited pen registers not obtained in conformity with the statute, *see* 18 U.S.C. § 3121(a)) was governed solely by, and consistent with, the Fourth Amendment. That decision simply did not address the propriety of obtaining the order under the All Writs Act. *See* 654 F. Supp at 405. *Videotapes* and *Doe* both involved the use of an investigative technique in the service of bringing a charged fugitive before the court. *See Videotapes*, 2003 WL 22053105 at *1 (noting that the requested relief was sought "in order to locate defendant Y and to execute a warrant for the arrest of

defendant Y previously issued by a judge of this Court"); *Doe*, 537 F. Supp at 839.[23] Such circumstances plainly warrant use of the All Writs Act in aid of the court's jurisdiction in a way that a request for cell site information – or the request to use any investigative technique in furtherance of a criminal investigation prior to the issuance of charges – does not.[24]

Second, none of the cited cases relied on the All Writs Act to trump existing statutory law governing the use of investigative techniques, nor did any of them purport to fill a gap in an existing statutory scheme. The closest that any of the cited cases come to such usage is *Mosko*, which, as noted above, simply does not address the propriety of so applying the All Writs Act.

---

[23] In this regard, I note that the government's quotation from *Doe* is misleading in a material respect. The government writes: "This power to issue supplemental orders in aid of the court's jurisdiction 'extends to persons who are not defendants and have not obstructed justice.'" Reply at 8 (citing 537 F. Supp. at 838 (although the correct citation is to page 839)). The reader of that quotation (replete with the unbracketed period inside the quotation marks) could be excused for thinking that it announced a broad power under the All Writs Act that extends to circumstances where no prior court order is to be vindicated. But the government omits that the court in *Doe* continued the quoted sentence to make clear that the statute's reach extends to such persons "if their assistance is needed to effectuate a prior order of the court and the assistance required is not burdensome." 537 F. Supp. at 839. Given that the issue before me is whether the All Writs Act supplies authority to the executive branch to conduct its own criminal investigation rather than to assure compliance with a court order, the government's omission – and it's failure to signal that omission in any way – is misleading.

[24] The only other specific example that the government calls to my attention is its use of the All Writs Act to secure, on the basis of a showing of relevance to a criminal investigation, "hotwatch" orders that "direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction." Reply at 8-9. The government cites no decision approving the use of the All Writs Act for such purposes, nor does it specify whether such orders are typically used to hunt fugitives or instead for the investigation of non-fugitives who are suspected of committing a crime but not yet charged. The propriety of the latter use of the All Writs Act is not before me, and the former kind of use would be entirely consistent with *Doe* and *Videotapes*. The example therefore has no impact on my analysis.

Thus, as far as I can tell, the government proposes that I use the All Writs Act in an entirely unprecedented way. To appreciate just how unprecedented the argument is, it is necessary to recognize that the government need only run this Hail Mary play if its arguments under the electronic surveillance and disclosure statutes fail. *See* Reply at 8 ("Lastly, were additional authority required ... the Court has authority under the All Writs Act"). But if, as explained above, those statutes do not authorize the acquisition of cell site information on a showing less exacting than probable cause, there is no way I can plausibly decide that ordering such relief is even consistent with principles of law, let alone in aid of them. *Cf.* 28 U.S.C. § 1651 (authorizing the issuance of "all writs necessary or appropriate in aid of [the courts'] respective jurisdictions and agreeable to the usages and principles of law").

The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.

III. Conclusion

Resolution of the government's motion for reconsideration has proved so difficult because Congress – which has on several occasions taken pains to update the laws regulating electronic surveillance so as to reflect advancing technology – has simply not addressed the matter now before me. The instant exercise is thus not a matter of discerning how Congress has decided the issue, for it has not. Rather, it is a matter of interpolation, for which there are two reasonable

approaches. First, a court can seek to determine whether and how the statutory language that Congress has enacted, in deciding other questions of electronic surveillance policy, answers the question. Second, a court can endeavor to understand the matrix of policy decisions that are reflected in the laws that Congress has passed and then strive to determine, against that backdrop, how Congress would likely resolve the question at hand.

Neither approach by itself is fully satisfactory. The first risks the judicial creation of law that is unintended or, worse, contrary to legislative intent. The second begs policy questions that judges have no particular competence to determine (including the threshold matter of identifying the particular Congress – the one that enacted CALEA? the one that last amended the Pen/Trap Statute? the one sitting today? – whose likely intentions the court should attempt to divine). While neither approach alone offers much comfort, in the absence of a clear Congressional mandate a court could do worse than to embrace a result that is favored by both approaches. I find that to be the case here. Neither the letter of the law nor its spirit compels, or even permits, the relief the government now seeks.

Accordingly, for the reasons set forth above, I conclude that some of the analysis in the August Order was flawed, but that the result was nevertheless correct. The applicable statutes allow the government to obtain historical cell site information on the basis of a showing less exacting than probable cause, but do not allow it to obtain such information prospectively on a real-time basis. When the government seeks to turn a mobile telephone into a means for contemporaneously tracking the movements of its user, the delicately balanced compromise that Congress has forged between effective law enforcement and individual privacy requires a showing of probable cause. Or at least, that is the best answer I can discern in a statutory scheme

that is anything but clear. That is why, grateful as I am for this opportunity to correct and refine my reasoning, I continue to urge the government to seek appropriate review of my decision in a forum that can provide more authoritative guidance on this important matter.

SO ORDERED.

Dated: Central Islip, New York
October 24, 2005

/s/ James Orenstein
JAMES ORENSTEIN
U.S. Magistrate Judge